EXHIBIT A

XYZ ORGANIZATION BUSINESS ASSOCIATE DATA SECURITY PLAN

1. **State the nature of the requesting organization's relationship with DMAS. In the absence of a Business Associate Agreement or some other formal contractual relationship with DMAS, please provide an explanation of how the proposed use of DMAS data is directly related to State Plan Administration (see 42 CFR, Section 431.302).**

   XYZ is the contractor for DMAS contract # XXXX_XX for Preauthorization and Utilization Management Services.

2. **Provide the name of the Business Associate's designated Information Security Officer, including full name, address, phone number and fax number. State the individual's relation to the business function.**

   Name
   Title
   Organization
   Address
   Phone
   Fax

   Ms. Doe oversees all IT operations at XYZ including connectivity to and data transfer between the DMAS Medicaid Management Information System (MMIS) and XYZ.

3. **Provide the names and position designations of all individuals who will have access to the data at or for the Business Associate.**

   Associates' name, title, department

4. **State the exact purpose(s) for which data will be used.**

   1) Medical Review
   2) Report Generation

5. **Describe the format (e.g., tape, paper, disk) in which the Business Associate envisions receiving the required data from DMAS.**

   Data is submitted from providers by telephone, fax, or mail for medical review purposes and is entered into the internal XYZ databases. Information for all review cases is stored on a XYZ Windows 2000 based server with Oracle 8i as

the database management system. Data are backed up to magnetic tape at the end of each business day and stored offsite at X location.

6. **Describe the medium within the Business Associate's organization upon which the data will be stored (e.g., will the data be on a disk pack accessible by the Business Associate's mainframe; will the data reside on a floppy disk stored in a box of similar disks beside the Business Associate's PC; will the data be accessible to many users through a network on the Internet or on an Intranet?)**

   To ensure confidentiality and security, XYZ maintains a filing process that includes staff assigned for file maintenance, file retrieval, file purging and file preparation for offsite storage. XYZ provides DMAS with access to all files during normal hours of operation.

   XYZ maintains file storage facilities for on-site review of the previous six months of documentation. XYZ maintains offsite storage for files older than 6 months at X storage facility. Files stored at this facility are returned to our location within 24 hours of the retrieval request. Emergency same-day retrieval service is also available.

   Information pertaining to all requests is entered at the Windows 2000 desktop using Visual Basic developed screens and is stored on our Windows 2000 based server with Oracle 8i as the database management system. Data is backed up to magnetic tape at the end of each business day and stored offsite at x location. Access to the server for administrative purposes is limited to the Systems Manager, John Doe, and the Database Administrator, Jane Doe. User access to the system and the case review data is controlled by Windows 2000 security provisions with additional access limitation imposed on the database side via Oracle. Both user ID's and passwords are required for access. Passwords are automatically aged by the system and must be changed by each user every thirty (30) days.

   The Virginia Medicaid system is housed on a Hewlett Packard Pentium III 600 MHz server with 384k memory. Hard disk storage includes a RAID-5 disk array with four – 9.1 KB disk drives, a redundant power supply and tape backup. This system will have the same connectivity to DMAS MMIS as described above.

   Data are never sent over the Internet. XYZ uses a secure 'internal' email system. Connectivity to our network is through a LAN in our Richmond office that then accesses our corporate email server via a dedicated frame delay connection line. We do not use Internet email facilities to send any DMAS information. Please refer to the response to question 7 for further information.

   XYZ currently connects to the MMIS at x location via a frame-relay connection from our Richmond office to DMAS.

EXHIBIT A

Future Operating Environment

As required by our new contract with DMAS we will eventually connect to MMIS at X location directly, rather than connecting at DMAS. We will use a serial connection between the XYZ provided CSU/DSU and the X router. Based on the expected volume, we will provide a 64 KBPS frame relay dedicated data line to the current DMAS Fiscal Agent's data center. In the event that traffic increases significantly, additional bandwidth can be added. At both ends of the frame relay data line, XYZ will provide an ADTRAN TSU LT T1/Fractional T1 CSU/DSU. A public address subnet will be provided if requested by Fiscal Agent for router-to-router connection. There will be a serial router port connection to the CSU/DSU on the Fiscal Agent side of the connection. As required, only public IP addresses will be presented across the data line. No connections across the Internet will be used.

XYZ will employ terminal emulation software – Eicon Access for Windows 3270 – to access the system from our desktop personal computers. Our existing employees and the DMAS contract monitors currently use this software to provide 3270 emulation for access to the DMAS computer system.

While our existing computer system easily and effectively handles all the processing required to support the DMAS requirements, every automated system can be improved. To reduce our maintenance costs, improve system access to DMAS authorized users and improve reliability, we are enhancing our existing Visual Basic/Oracle 8i Based computer system to a configuration that can also employ a browser-based client under Windows 95/98/2000. This browser-based access will use a secure Virtual Private Network (VPN) connection to XYZ's Windows 2000 server supporting the Oracle 8i-database management system. This new environment will make it possible to extend access to the system to any DMAS approved user with access to the Internet, subject to encryption in the manner prescribed in the HCFA Internet Security Policy dated 11/24/1998.

Based on provider interest and approval of DMAS, we will develop ASP based forms to allow providers using their Internet connection to enter data about the pre-authorization request directly from their location – reducing or eliminating the need to fax this information to XYZ. Entry of information by the providers at the source of data to the XYZ maintained database means that errors and processing time associated with printing the fax, routing the fax to the appropriate reviewer and subsequent entry of the information to our computer system are eliminated.

7. **Describe the provisions the Business Associate is taking to physically safeguard DMAS data in whatever form it has been provided or created. As part of the Business Associate Data Security Plan for DMAS, the Business Associate must include a copy of any security plan, security policies, or security procedures currently in effect within the organization.**

EXHIBIT A

Our data security and confidentiality plans are summarized and described below.

XYZ is well aware of the confidential nature of the information that we will receive and process, both in paper and electronic format. We also understand that all data provided by DMAS to XYZ remains the property of DMAS. We will use this data only for the activities needed to fully support all the requirements of this scope of work. In the event a need arises for use of the DMAS provided data for some other purpose, XYZ will obtain written permission from DMAS in advance of any use of this data. XYZ also agrees to follow federal and state confidentiality requirements as set forth in the then current Code of Federal Regulations and the then current Code of Virginia.

To ensure XYZ compliance with all of the confidentiality and security requirements associated with use and storage of health care information, all XYZ employees must adhere to the confidentiality rules and security procedures outlined in the XYZ Employee Notebook.

The notebook is updated as needed but at least every year to reflect current XYZ policies that its employees must adhere to. Every new employee is provided with a copy of the manual, and our Human Resources Department reviews the key section dealing with our confidentiality policy. This section includes information about:

- Access and disclosure of confidential information
- Responsibility for confidentiality vested in a single individual
- Research and statistical reporting
- Legal requests for information
- Disclosure, monitoring, review and evaluation
- Disclosure of privileged data and information to third parties
- Patient access to XYZ data and information
- Prospective employee background investigations
- Trustee and employee access and training
- Document accountability
- Building security
- Communications security, ADP security
- Subcontract requirements
- Responsibilities of medical review coordinators
- Requests for the generation of non-privileged information
- Penalties for disclosure of confidential information

HIPAA mandates new security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. The standard mandates safeguards for physical storage and maintenance, transmission and access to individual health information regardless of the medium used. In addition to our

institutionalization of confidentiality and security policies discussed above, XYZ will comply with all HIPAA data security requirements as needed.
These are some examples of steps we already have in place in:

- We have in place appropriate physical safeguards to protect data integrity, confidentiality and availability. Our offices are secure and require a key or swipe card for entry. Only XYZ employees and four DMAS contract monitors are granted these keys/cards. Visitors to XYZ facilities are required to register and wear visitor's passes. In addition a XYZ employee must escort them. Our computer servers and databases are housed in a locked room within our secure facility. Access to the computer room is limited to information technology personnel. XYZ employees escort maintenance personnel at all times. Smoke detectors and automated sprinkler systems are installed to protect from fire.

- We have developed and implemented administrative procedures to guard data integrity, confidentiality and availability. All employees are required to read and sign a non-disclosure agreement as a condition of employment. An employee handbook has been developed that details all employee responsibilities and acceptable conduct and the actions that may be taken in the event of improper conduct. Security awareness training is conducted periodically. All data is backed up on a daily basis and secured in a fireproof safe. Virus detection and correction software is installed on all PCs and corporate servers. Updates to this software are made on a bi-weekly basis.

- We have implemented technical security services to guard data integrity, confidentiality and availability. Access to our local area network and the services available on that network are limited to authorized users. The program manager for each program grants authorization and a unique user id and password are used to gain access. Passwords are automatically retired every thirty (30) days. Access to the automated applications and underlying databases requires a separate logon and password. Access is further controlled on a "need" basis, providing either no access, read only, or write access to data. Users are automatically denied access following 3 failed logon attempts. System logs record user logon attempts, and applications capture information about who has added, modified or deleted records.

- Finally we have implemented appropriate technical security mechanisms that include the processes to prevent unauthorized access to data that is transmitted over a communications network. Our Systems Administrator, who grants access to users only upon program manager approval, controls access to our network. Currently, remote access to our local area network (and thence to the applications and databases) is highly restricted, and is used only from system administration. As we migrate our applications to a "web" ready environment, we will only support dial-in access (to users approved by DMAS) via a limited number of dial up circuits or via the Internet using Virtual Private Network (VPN) technology. VPN supports user authentication via public-

private key exchange and provides a secure connection from the remote user to our systems over an encrypted "virtual tunnel" through the Internet.

To ensure that our security policies and practices remain current, we will periodically assess our security risks and vulnerabilities and the mechanisms currently in place to mitigate those risks and vulnerabilities. Measures in addition to those described above will be added as needed.

8. **Identify all individuals (or entities) to whom the data will be distributed as a result of the business function.**

   Data that identify individual recipients, providers or facilities will never be distributed to any entity outside DMAS except with the express prior consent of DMAS. Aggregated data may be used for provider training, legislative presentations etc., but also only with the prior consent of DMAS. Data may occasionally be requested by HCFA or to other federal oversight authorities for inclusion in multi-state studies, analyses or for other purposes, but again, will not be released without the consent of DMAS.

9. **Describe through what mechanisms and in what format the Business Associate proposes to make final work products available to DMAS.**

   XYZ will use the mechanisms and formats preferred by DMAS to make final work products available. This may include electronic transmission, tape, diskette, hard copy, or any other medium requested by DMAS.

   Currently the weekly, monthly, quarterly annual and ad hoc reports are sent to DMAS electronically and/or in hard copy format. XYZ does not electronically send any reports to DMAS that contain patient identifiable information.

10. **Summarize, within the Business Associate Data Security Plan, the data retention and disposal requirements that exist in the Contract or Agreements with DMAS. If the Business Associate is subject to any other retention requirements, those requirements should be included in the Business Associate Data Security Plan.**

    To ensure confidentiality and security, XYZ maintains a filing process that includes staff assigned for file maintenance, file retrieval, file purging and file preparation for offsite storage. XYZ provides DMAS with access to all files during normal hours of operation.

    XYZ currently maintains file storage facilities onsite and available for review for the previous 6 months of documentation. XYZ maintains offsite storage for files older than 6 months at x storage facility. Files stored at this facility are returned to our location within 24 hours of the retrieval request. Emergency same-day retrieval service is also available.

EXHIBIT A

XYZ shreds all hard copy data that is not stored for retrieval. Any removable magnetic media that has been used for storage is degausses before disposal.

11. Provide a statement of acknowledgement in the Business Associate Data Security Plan that all DMAS data, no matter how manipulated or summarized remains the property of DMAS.

XYZ is well aware of the confidential nature of the information that we will receive and process, both in paper and electronic format. We also understand that all data provided by DMAS to XYZ remains the property of DMAS. We will use this data only for the activities needed to fully support all the requirements of this scope of work. In the event a need arises for use of the DMAS provided data for some other purpose, XYZ will obtain written permission from DMAS in advance of any use of this data. XYZ also agrees to follow federal and state confidentiality requirements as set forth in the then current Code of Federal Regulations and the then current Code of Virginia.

12. Describe the provisions the Business Associate is taking to ensure continuity of service to DMAS in the event of an emergency or other catastrophic event causing Business Associate business interruption (where applicable).

XYZ has instituted a policy detailing our procedures for preauthorization during loss of connectivity. The following policies may be found in our XYZ -- Virginia Operations Policy and Procedures Manual and are also attached to this document.

- Utilization Review (Inpatient) Procedure for Loss of Connectivity.
- Utilization Management (Inpatient) Procedure for Loss of XYZ Database
- Prior-Authorization (Outpatient) Procedure for Loss of Connectivity
- Prior-Authorization (Outpatient) Procedure for Loss of XYZ Database
- Behavioral Health Review Procedure for Loss of Connectivity
- Behavioral Health Review Procedure for Loss of XYZ Database
- Community Based Care Review Procedure for Loss of Connectivity
- Community Based Care Review Procedure for Loss or XYZ Database

13. Note the existence of any insurance or bonds carried by the Business Associate, which would protect the Business Associate and DMAS from contingent liability in the use of the data. Otherwise, provide a statement in the Business Associate Data Security Plan if no such insurance coverage exists.

Our current Managed Care E&O Policy does cover “Medical Information Protection for claims arising out of the inadvertent release of medical information/records.” Our underwriter is:

Name

EXHIBIT A

Title
Organization
Address
License #
Phone
Fax

Attachments:

Enclosed are additional documents including Policies and Procedures that XYZ has issued in order to meet the guidelines of the Data Security Plan.